UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,918	01/26/2004	Michael F. Angelo	200314543-1	2632

22879 7590 05/30/2008
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
DOAN, DUC T	
ART UNIT	**PAPER NUMBER**
2188	
NOTIFICATION DATE	**DELIVERY MODE**
05/30/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10764918
Filing Date: January, 26 2004
Appellant(s): ANGELO, MICHEAL F.

Micheal G. Fletcher Reg #32777
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/25/2008 appealing from the Office action mailed 9/21/2007.

(1) Real Party in interest

A statement identifying by name the real party interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US Pub 2003/0174842	Challener	09-2003
US Application 10764918	Angelo et al	01-2004

US 7187771	Dickenson et al	03-2007

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejection 35 USC 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 8-13 and 14-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 8 and 14 are directed to a security module which is a software/program (see specification's paragraph 21). Therefore, the claimed invention is directed to non-statutory subject matter.

All dependent claims are rejected as having the same deficiencies as the claims they depend from.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject

> matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-26, 31, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Appellant's admitted prior art (APA) and in view of Challener (US Pub 2003/0174842).

As in claim 1, APA discloses a method of operating security modules in a computer including having a first security module and a second security module both of them are configured to perform the same functions, that is the functions associating with a security module (APA's paragraph 4, two security modules configured to perform the same security functions such as encrypting, sealing etc..).

APA does not disclose the claim's details associating with the keys of security modules, However, Challener'842 describes a method for storing private key of one security in another security module using establish standard such as TCPA (Challener's paragraph 6, lines 1-10) comprising the acts of: detecting a second security module in the computer; determining whether a key associated with the second security module is available to the first security module (Challener'842's paragraph 28, Fig 3: #54 query whether user's private key is stored on the TCM server, Fig 1: #40 that corresponds to the claim's first security module); and obtaining the key associated with the second security module if the key associated with the second security module is not stored at the first security module (Challener'842's paragraph 28, server obtains the private key from the client's security module, Fig 1: #54 that corresponds to the claim's second security module, Fig 1: #22; Challener's paragraph 12 discloses that the first security module, TCM server Fig 1: #40, obtaining the private key associating with the second security module, Fig 1: #22, and providing this key information to a client/user. Obviously, if this key has not been stored at the first security module, the first security module, server, will obtain it from the client's computer and save it for future referencing, in a migrating manner, see Fig 4a, and paragraph 32).

It would have been obvious to one of ordinary skill in the art at the time of invention to include the method and associating apparatus for storing private key of one security in another security module using establish standard such as TCPA in APA's system, thereby the private key of one security module can be retrieved from another security safely with any computers enable with established standard such as TCPA (see Challener's paragraph 8).

As in claim 2, Challener further discloses wherein each of the first security module and the second security module is a trusted platform module ("TPM") (Challener'842's paragraph 26 describes the server TPM Fig 1: # 40 including modules conforming to the trusted platform module specification (see Challener'842's paragraph 6); Challener'842 paragraph 12 further disclose the TCPA is employed in the second security module, for example Fig 1: #22).

As in claim 3, Challener'842's paragraph 28 further describes comprising the act of requesting the key from the second security module (claim 3; requesting private key from client's system Fig 1: 312).

As in claim 4, Challener further discloses the act of sending a public key from the first security module to the second security module if the key associated with the second security module is not stored at the first security module (Challener'842's paragraph 28 discloses when the user's private key is not stored in the first security module (Fig 1: #40 TPM server), the server Obviously send the public key (public non-migratable key of the server) to the second security module which being used to "wrap" the private key, and the second security module sends this wrapped information back to the TPM server).

As in claim 5, Challener further discloses the act of sending a public key along with validation information from the first security module to the second security module if the key associated with the second security module is not stored at the first security module (Challener'842's paragraph 31 discloses for both the requesting and responding messages, additional information to validating the messages can be sent along, for example, information associating with authorization for the sender of messages) .

As in claim 6, Challener further discloses the act of storing the key in a memory associated with the first security module (Challener'842 Fig 1: #48, #50).

As in claim 7, Challener further discloses the act of defining the key to be a private key (Challener'842's paragraphs 24, 27).

Claims 8, 14, 21, and 31 are rejected based on the same rationale as in the rejection of claim 1.

Claims 9, 15, 22, and 32 are rejected based on the same rationale as in the rejection of claim 2.

Claims 10, 16, and 23 are rejected based on the same rationale as in the rejection of claim 3.

Claims 11-12, 17-18, and 24-25 are rejected based on the same rationale as in the rejection of claims 4-5 respectively.

Claim 19 is rejected based on the same rationale as in the rejection of claim 6.

Claims 13, 20, and 26 are rejected based on the same rationale as in the rejection of claim 7.

Claims 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over APA and Challener (US Pub 2003/0174842) as applied to claims 1 and 8 respectively, and in view of Dickinson et al (US 7187771).

As in claim 33 Challener further discloses comprising the act of accessing data encrypted by the second security module using the key associated with the second security module (Challener discloses a method in which a first security module (Fig 1: #40) can access data encrypted by the second security module using the key associated with second security module (Challener's Fig 3: #60-64, paragraph 31, the stored private key (corresponding to the claim's data) is encrypted using non-migratable public key (corresponding to the claim's key associating with the second security module), and returning the user's private key/data to the client). In other words, Challener teaches a method in which a first security module can retrieve a data associating with the second security module by using the stored key associated with the second security module and presenting the data to the user. APA and Challener do not expressly disclose the aspect of the claim's regarding the failure of the second security module. However, Dickinson discloses a method in which important data is controlled by security/trust module logic (see Abstract, Fig 2). Dickinson further discloses that the security/trust system comprises several redundancy engines authenticate engines, trusted engines (see Dickenson's column 5 lines 60-67, column 13 line 46 to column 14 line 3, trust engines perform authenticate functions), which control several redundant copy of critical data, such that the failure of one module/one component would not affect the overall security system. It would have been obvious to one of ordinary skill in the art at the time of invention to include the redundant method for storing copies of data controlled by redundant security/trusted modules in APA's system modified by Challener and thereby if one of the security module fails, the data can be obtained from the remaining security modules and other copies of data (see Dickinson's column 17 lines 46-61).

Claim 34 is rejected based on the same rationale as of claim 33.

(10) Response to Argument

Appellant's arguments in response to the last office action have been fully considered but they are not persuasive. Examiner respectfully traverses Appellant's arguments for the following reasons:

A) Appellant's argument with regard to the rejection of claims 8-13 and 14-20 under 35 U.S.C 101 is not persuasive.

Appellant argues " In particular independent claims 8 and 14 are each directed to "[a] first security module in a computer" and recite discrete physical structures in the bodies of the respective claims. Specifically, the body of claim 8 recites, "a *detector* that is adapted to detect another security module.., *and a device* that obtains at least one key." (Emphasis added). The body of claim 14 recites, *"means for detecting* another security module...means *for determining* whether a key associated with the other security module is stored at the first security module; and *means for obtaining* the key." (Emphasis added).."

Essentially, Appellant argues that independent claims 8 and 14 do not have 35 U.S.C 101 issue because certain physical structures are recited and being claimed. The physical structures according to Appellant, are items being emphasized in above paragraph, **"a detector" "a device"** in claim 8 and **"mean for detecting"** , **"mean for obtaining"** in claim 14.

In response, specification's paragraph 21 clearly states that the detection and the key could be merely some code/software ("the detection 82 and the key obtaining device 84 may be implement in hardware, **software**, or any combination thereof"). And because these only two structures are claimed in the body, and both of them (the detector and the device) can be implemented as software only as stated in the specification. Thus the claim does not have any physical structure being claimed and fails to fall within the statutory of invention;

Examiner further notes, Even though the rebuttable pre-assumption that 35 U.S.C 112 sixth paragraph applied in the claim interpretation of "mean for detecting" and "mean for obtaining," corresponding "structures" in the disclosure is not automatically and inherently limited to hardware-inclusive embodiments.

Appellant further argues, "Moreover, the specification clearly describes the security modules as including physical structure. *See, e.g.,* FIG. 3; paragraph 28, lines 3-4 (stating "the first TPM 143 **may** include an input/output interface, *a processor, and a memory* 156 that is used to store TPM keys 158" (Emphasis added)). Accordingly, the subject matter of independent claims 8 and 14 clearly contemplated to include tangible hardware elements, as well as software."

In response, Examiner notes that paragraph 28, lines 3-4 can be interpreted as the TPM may or **may not** have any of elements such as input/output interface, a processor and a memory 156 that is used to store TPM keys 156. In other words, Appellant quoted a specification paragraph which clearly states that the TPM does not necessary require to have a memory or keys stored in a memory . Thus, keys are not necessary required as a part of the TPM as discussed, and the keys are not explicitly claimed as in the current claims 8 and 14. Therefore, Examiner maintains that the body of the claims only has two structures, "a detector" and "a device", both of them could be merely software and claims fail to fall within the statutory category. Thus, the argument is not persuasive.

B) Appellant's argument with regard to the rejection of claims 1-26,31 and 32 under 35 U.S.C 103(a) is not persuasive.

1) With regard to argument for the rejections of independent claims 1,8,14,21 and 31,

Appellant argues that Examiner cannot use the information disclosed in section background of the related art of the instant application as the admitted prior art just because Appellant put in a disclaimer statement, "it should be understood that these statements are to be read in this light, and not as admission of prior art".

In response, Examiner has carefully reviewed the background of the relate art and believe this section clearly teaches the facts that have been known in the field of computer system including multiple security modules in a single computer system (paragraphs 3 and 4) and multiple security modules are doing the same functions. For example, APA teaches commonly known functions that every security module must such as encrypting and decrypting data with proper keys, paragraph 3 lines 6-7. And of course, security modules in a computer system must carries out all same commonly known functions such as encrypting and decrypting data (paragraph 2 lines 5-7).

Examiner would like further to point out that **the computer environment of a computer having two security modules is known in the art**. APA teaches such a computer/computer environment (paragraph 3, "however if multiple security modules are utilized in a single computer system, different modules may seal computer).

Dickenson US patent 7187771 (herein Dickenson) is referred to show as another evident that the above computer/computer environment is known in the art. Specifically, Dickenson teaches that a trust engine in a server (a computer) , column 2 lines 31-42, in one embodiment can comprises of several instants of trust engines (several security/trust modules) or in another embodiment comprises a redundancy module (i.e server/computer comprises a security/trust module and a redundancy security/trust module, i.e two security/trust modules in a single computer), such that the overall system can operate if one of the security/trust module fails (column 5 lines 60-67).

In other words, Dickenson teaches a single computer/computer environment, same as of APA, comprises a computer having several security/trust modules. Dickenson further teaches the well known principle of redundancy, that is by using two or more security module in redundancy manner, the overall system can still operate even if one of the security module temporary not operating/failing (column 5 lines 60-67).

In addition, regarding Appellant's argument, "..Appellant put in a disclaimer statement, "it should be understood that these statements are to be read in this light, and not as admission of prior art". It's noted that the above statement is merely an allegation and overall disclaimer statement. Appellant fails to provide any specific evident to support a computer system with two is not a known fact in the art.

Therefore Appellant's argument is not persuasive.

Appellant further argues that "Moreover, even if the portions of the instant application which were cited by the Examiner were considered to be prior art, *a prima facie* case of obviousness has not been presented. Specifically, while the portion of the instant application cited by the Examiner discloses two security modules in a computer system, it does not disclose that they are configured to perform the same functions. Furthermore, the Challener reference fails to disclose this feature. In particular, the Challener reference discloses a system wherein two security modules in two different computers perform different functions. For example, one security module located in the server is configured to collect keys from and distribute keys to client computers, while a second security module located in a client computer may generate keys, provide keys to the security module of the sever and access the keys stored at the server to allow for the free-seating of a user within the network environment. *See* Challener, paragraphs 11 and 12. As such, not only are the security modules in separate computers, but they do not perform the same functions". Examiner disagrees.

In response,

First, Appellant's argument regarding " function" appears to mischaracterize between the functions of the security modules and the details steps of the functions done by different actors. The functions of security modules can be defined in the architected document of a certain trust module platform, for example a security module is defined having functions such as hashing, asymmetrical key encryption/decryption for generating keys and obtaining keys etc... And any security module must have the **same functions** as stated in the architected document of a certain trust platform module, so that they can interoperate among themselves. However, the security modules having same functions (keys generating, key obtaining functions) do not mean they must execute same details steps when interact among themselves. For example, to obtain the key, a security module/actor acts as requester of the key must uses steps of a requester/client different with another security module/actor acts as a provider/sever of the key. Therefore Appellant is misleading by argue Challener not teaching the same functions. In fact, Challener 's paragraph 6 teaches all security modules having the same functions conforming to a TCPA platform architecture, such that they can interoperate among themselves whether one security module acts as client (requesting the key) and another security module acts as server (providing the key).

Second, Appellant argues, "Challener reference does not disclose, teach, suggest or provide any motivation with respect to providing multiple security modules in the same computer". The employment of several security modules in the same computer such that if one security module is not available, the overall system can operate with another security module is well known and taught by APA and Dickensen in above paragraphs. Examiner only relies on Challener for the teaching the retrieving of key and thus retrieving of key and associated data can be done independent of the security modules, **whether or not the security modules are in the same computer or in different computers.** And one skill in the art would at the time of invention would recognize the way to retrieve key independent of security modules as taught by Challener and applied to APA system, and thereby further allowing the key and the associated data can be retrieved easily by any security module and in a safely manner using functions established in standard such as TCPA (see Challener's paragraph 8).

Third, Examiner further submits that Appellant's arguments regarding of different acts between the requester and the provider is irrelevant simply because there is not any limitation in the claim describing how the keys are provided, let alone arguing of different acts with the requester and the provider.

Thus Examiner submits that the recited references teaching all the steps as claimed. Therefore, Appellant argument is not persuasive.

2) With regard to the argument for the rejections of dependent claims 5,12,18 and 25.

Appellant argues, "Challener reference cited by the Examiner does not even mention public keys, much less the sending of "public keys along with validation information". Examiner disagrees.

Challener paragraph 31 clearly teaches additional information can be send along, "transmitting authorization data" , corresponding to claim's validation information. Challener paragraph 28 teaches sending along a public key, "the private key is wrapped with a public non-migratable key". Therefore, Appellant argument is not persuasive.

C) Appellant's argument with regard to the rejection of claims 33 and 34 under 35 U.S.C 103(a) is not persuasive.

Appellant argues, "...However, Appellant security, *Id.* at col. 31, line 56 through col. 32, line 14. However, Appellants are unaware of, and the Examiner has not cited to, any portion of the Dickinson reference that can reasonably be considered to disclose multiple security modules in a single computer....".

In response, Examiner relies on Dickinson's for teaching a concept of redundant of security/trust engines so that the overall system can operate if one of the security/trust engine fails (column 5 lines 60-67). Specifically, Dickenson teaches that a trust engine in a server (a computer) , column 2 lines 31-42, Dickenson further teaches the server (a computer) trust engine in one embodiment comprises of several instants of trust engines or in another embodiment comprises a redundancy module (i.e server/computer comprises a trust module and a redundancy trust module, see Dickenson's column 3 lines 12-19), such that the overall system can operate if one of the security/trust engine fails (column 5 lines 60-67).

In other words, Dickenson teaches a computer/computer environment, same as APA, comprises a computer having several trust modules. Dickenson further teaches that one of the security module can be used in a redundant manner, so that the overall system can operate if one of the security/trust engine/module fails (column 5 lines 60-67).

Therefore, Appellant argument is not persuasive.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/ Duc T. Doan/
Duc T. Doan
Examiner, Art Unit 2188

Conferees:

/Hyung S Sough/
Supervisory Patent Examiner, Art Unit 2188
05/26/08

/Kevin L Ellis/
Acting SPE of Art Unit 2187
5/27/08